A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture

László Bokor, Zoltán Faigl, Sándor Imre
Mobile Innovation Centre, Budapest University of Technology and Economics
Bertalan Lajos u. 2, H-1111, Budapest, Hungary
{goodzi, zfaigl, imre}@mik.bme.hu

***Abstract*—The Ultra Flat Architecture is a new concept of fixed-mobile convergent networks that aims to scale well with the mobile Internet traffic explosion prognosticated for the next 5–10 years. This paper presents a new delegation-based UFA signaling framework using HIP, IEEE 802.21 and the context transfer protocol. The main procedures contributed by this signaling framework are terminal attachment, session establishment, proactive handover preparation and handover execution services. The paper introduces several novel Host Identity Protocol extensions, i.e., two different HIP delegation service types for optimized message exchange in HIP-based UFA mobility and multihoming operations, a context transfer scheme for HIP and IPsec associations supporting and extending the mechanisms of the delegation-based UFA functions, and a fast operator-centric method for HIP-level access authorization. The proposed UFA signaling framework is compared with the existing SIP-based UFA signaling solution. The comparison shows that our scheme is able to support legacy Internet applications in an operator based environment, it is stronger in security, but its deployment requires more additional modules in the architecture. For IMS applications, the SIP-based alternative is a better choice.**

***Index Terms*—scalability, Ultra Flat Architecture, Host Identity Protocol, fast access authorization method for HIP, HIP delegation services, HIP context transfer, IEEE 802.21, CXTP**

I. Introduction

Current trends in mobile telecommunication show rapid growth of Internet related services and ever growing demand for them. More and more users are willing to access the Internet from their portable devices. Mobile subscribers prefer flat-rate, unlimited traffic plans and want uninterrupted, ubiquitous access to their everyday Internet applications anytime and anywhere. To satisfy the demands, operators are going to use heterogeneous access technologies: WiFi, WiMAX, GERAN, UTRAN, HSPA, LTE, LTE-A will coexist very soon in most European countries. This heterogeneity must be transparent as users would like to witness seamless, QoS-aware and secure maintenance of their ongoing sessions and active states during locator (e.g., IP address) changes due to any kind of horizontal or vertical handover situation. As a result, the main challenges for mobile networks and their operators in the forthcoming years will be 1) to offer high bitrate data services for the continuously growing mass of fixed-mobile convergence customers, 2) to provide seamless transition between heterogeneous access technologies and 3) to support advanced mobility and multihoming scenarios like network mobility, session mobility, simultaneous multiaccess or per-application mobility.

It is highly expected that due to their centralized (anchor-based) design, mobile architectures currently being under deployment or standardization would not scale particularly well to efficiently handle all the above challenges. It is also anticipated that mobility management tasks of advanced scenarios cannot be tackled effectively if IP address will continue to remain both locator (for packet routing) and identifier (for referring to a host or session): the semantically overloaded nature of the Internet Protocol must be obviated by identifier/locator (ID/Loc) separation [1].

Motivated by the above reasoning, a novel mobile architecture should be created focusing on two main goals. On one hand bottlenecks from packet communication must be removed by eliminating user-plane anchors from the network and bringing IP routing close to the mobile terminals in means of physical location in the architecture. On the other hand service establishment, security and mobility procedures must be optimized by distributing them from centralized nodes and by introducing ID/Loc separation. Decentralized, robust, self-configuring and self-optimizing network structures are envisioned with reduced operation expenditure (OPEX), improved system capacity and energy efficiency. However the above mentioned reconstruction and optimization of current architectures seems to be inevitable, it cannot be implemented without strict attention to the compatibility with legacy applications and services, introducing a wide variety of new performance and functional constraints.

The basics of such a redesigned mobile architecture were firstly defined by Khadija Daoud et al. in [2], [3] and [4]. Their scheme is called Ultra Flat Architecture (UFA) since the number of network nodes is reduced to only one serving node called the UFA Gateway (UFA_GW) and traditional user and control plane functions are distributed in such UFA_GWs deployed at the edge of the architecture, close to the subscribers. The main characteristics of this proposal is that the execution of handovers is managed by the network via the Session Initiation Protocol (SIP) operating withing the frame of the IP Multimedia Subsystem (IMS). This SIP-based UFA session establishment and mobility management integrates QoS and allows network-control for optimization of resource consumption.

Even though SIP is a very powerful signaling solution for

UFA, it is not applicable for non-SIP (i.e., legacy Internet) applications and the published SIP-based UFA scheme also does not comply with ITU-T's recommendation of requirements for ID/Loc separation in future networks that allows the network layer to change locators or even protocols without troubling upper layer communication sessions [1]. Therefore, in this paper we present an alternative signaling scheme for the Ultra Flat Architecture based on the promising ID/Loc separation method called Host Identity Protocol (HIP). Our contribution in this paper lies in the design of a novel, HIP-based UFA signaling framework for managing network attachment, session establishment and mobility execution, and a possible way for integrating UFA with the IEEE 802.21 standard [5] for media independent handover initiation and preparation. We propose a two delegation service types for HIP, to reduce the number of HIP Base Exchanges (BEX) between the MN and the network and within the network. We provide a possible fast authentication method for HIP in operator-based environment by defining a new root key usage type, i.e., the HIP peer authorization root key. Our proposal is based on the assumption that an EAP-based L2 access authorization method providing Extended Master Session Key (EMSK) is performed in the UFA.

To introduce our proposal we first present the background of the work in Section II. This is followed by the fundamentals of the HIP-based Ultra Flat Architecture in Section III. As our design is based on a fast access authorization method for HIP layer, two novel HIP delegation service types, and on a CTXP based context transfer solution, we also introduce these in Section III. Section IV presents the main procedures of HIP-based UFA together with the integrated 802.21 mechanisms while Section V is devoted to compare our signaling scheme with the previously published SIP-based scheme. In Section VI we discuss some open issues of our proposal, conclude the paper and present future work.

II. Background

A. ID/Loc Separation

The inseparable bond between the locator and identifier functions of IP address (i.e., its dualistic behavior) makes it inconvenient or even impossible to design efficient and scalable mobility, multihoming, traffic engineering, routing and security solutions. Supporting heterogeneous network layer protocols or different locator families is also limited because of the same reason. The general concept of ID/Loc separation aims to eliminate the above problems and limitations by splitting the two roles of IP addresses and such allowing network layer to change locators without interfering with upper layer procedures. The concept gains more and more popularity: several different approaches exist for ID/Loc separation (e.g., LISP, SHIM6, FARA or HIP [6]) and it also has recently been introduced in the standardization activities of ITU-T for integration in future network architectures [1]. The common in all the above standards and recommendations is the use of distinct namespaces for both identifiers and locators with a dynamic mapping mechanism between them, making the duplicate role of IP addresses disappear. Some protocols (e.g., [6]) go even further and introduce special, cryptographically generated identifiers providing self-certification, hence easy authentication of identities even from frequently changing locations. Efficient AAA mechanisms can be designed based on this peculiar characteristic. Some solutions (e.g., [7]) also address scalability issues by eliminating anchor points needed for dynamic mapping, and introduce a new logical protocol layer as a distributed overlay for translating locators to identifiers.

B. A promising ID/Loc separation technique: HIP

In our proposed UFA signaling scheme we apply the Host Identity Protocol (HIP) that is an instance protocol providing a logical overlay for ID/Loc separation with cryptographic IDs (i.e., Host Identifiers - HIs) generated from a new, statistically globally unique namespace called Host Identity. In this namespace a Host Identifier is the public key of an asymmetric key-pair which is thus self-certifying, making possible the integration of strong security features such as authentication, confidentiality, integrity and protection against certain kind of Denial-of-Service (DoS) and Man-in-the-Middle (MitM) attacks. However, variable-length HIs are rarely used in HIP protocol packets, instead a 128 bit long hashed representation called the Host Identity Tag (HIT) is applied.

Several extensions have been defined to the base HIP protocol [6], e.g. advanced mobility and multihoming support, service registration [8], Rendezvous Server (RVS) extension [9], source address validation for authentication and access control, configuration provision [10] for merging HIP with DHCP, and relay mechanisms for NAT traversal. Together with other proposals for DHT-based distributed name services [11], [12] and overlay routing mechanisms [7], [13] HIP also enables tackling scalability issues of current architectures by reducing anchors.

C. IP Security

In HIP-based UFA framework, IPsec ESP in tunnel mode provides secure L3 transport for media and non-HIP signaling traffic. The inner addresses contain the identifiers of the traffic flow end-points, i.e., their HITs, while the outer addresses are locators of the IPsec tunnels that are on the path of the inner packet. We propose that in the UFA architecture traffic is transported through tunnel mode IPsec SAs. Tunnel mode IPsec SAs are established with HIP controls between the MNs and their UFA_GWs, between the communicating UFA_GWs, and the CNs and their UFA_GWs. Note that during the design of HIP-based signaling scheme for UFA, the Bound End-to-End Tunnel (BEET) [14] and Stripped End-to-End Tunnel (SEET) [15] modes were considered, but finally not applied. BEET mode supports ID/locator split frameworks, but not aimed for use cases where the locator (i.e., logically the outer address of an IPsec tunnel) and the identifier (i.e., logically the inner address) of the traffic flow belong to different network entities. SEET mode is a BEET (or other) mode IPsec ESP, but it is special for not covering the SPI value in the ESP

header with integrity protection. It is used in middleboxes (MBs) applying SPI translations on end-to-end IPsec ESP traffic flows. SEET mode could be used if end-to-end IPsec SAs were established between the MNs and CNs. In that case UFA_GWs should be considered as transparent MBs.

D. Context Transfer

Context transfers may facilitate fast handoffs, and reduce computational and network overhead. During the design of proactive handovers in HIP-based UFA, the trade-off was considered between state re-establishment and state transfer, and Context Transfer Protocol (CXTP) [16] has been chosen for the transfer of the states of certain HIP and IPsec associations between previous (pAR) and next access routers (nAR) during the handover execution procedure. In general, backward secrecy of keys in the contexts can be provided by one-way key derivations, forward secrecy should be optional using rekeying. The security of the CXTP messages is provided by IPsec. For seamless context transfer, we must tackle the collision due to occupied states on nAR (e.g., SPI collision), and the desynchronization of running states between the local and remote peers of the transfered association. Sequence and acknowledgment values for anti-replay protection and retransmissions might cause such issues, that could be handled by the adjustment of anti-replay window size. The transfer of IPsec and IKE contexts have been analyzed in [17]. Note that it is inevitable to apply delegation of HIP BEX rights from nAR to pAR, introduced in Section II-E and III-B2 because pAR must establish HIP association for nAR and the HIP peers, and pAR can only use its own private key for signatures. In our scheme, pAR and nAR are the source and target UFA_GWs (S_UFA_GW and T_UFA_GW), respectively.

E. Delegation of Rights

The delegation of signaling rights is motivated by the optimization of resource utilization between the delegator and the delegate. Delegates are temporarily authorized by the delegator to proceed in certain tasks, such as periodic location updates, rekeyings. The delegator may issue a public-key authorization certificate [18] to the delegate to proceed in his name at the peers. HMAC key could also be issued to a delegate in order to generate HMACs admitted by the peer, as described in [19]. Before right delegation it is important that the delegator establishes trust relationship with the delegate, i.e., the identity of the delegate must be authenticated. Delegation chains require implicit trust chains. In our signaling scheme, we apply public key authorization certificates containing the following information [18]:

$$\{K^{+}_{delegator}, K^{+}_{delegate}, roles, restrictions\}_{K^{-}_{delegator}} \quad (1)$$

F. Authorization and Accounting

Authorization, logging, and accounting of the usage of network resources is a basic requirement of operators. It raises the need for binding traffic flows to identities in MBs. If locators are used as identifiers, the identity theft becomes very easy, and binding flows to identities is hard. E.g., from security perspective, a NAT or NATP device [15] resembles a MiTM attacker, because translation between locators infers the replacement of the identifiers. It is required thus that MBs can cryptographically bind flows to identities. Several binding techniques exist for both transparent and non-transparent MBs, such as the verification of public-key signatures in control messages [15], [20], requiring signed responses to challenges added by the MBs to the flows [21], or hash-chain based methods [15], [20].

Non-transparent MBs are MBs that require registration and security association establishment from the peers. An alternative for both MB types is the verification of public-key signatures. Since identities and their public-key certificates are present in security control messages, data packets containing asymmetric signatures can be bound to identities [15], [20]. For Cryptographically Generated Addresses (CGAs) the identity is self-certifying, there is no need for certificate. Another binding technique for symmetric duplex communications is that MBs add challenges to the packets, and expect signed responses from the peers [21]. A method adequate for media flows is the hash-chain based binding [15], [20], but hash-chains are still vulnerable to the reuse of elements by on-the-path attackers, however duplications will be detected in the MB. Another important security requirement of operators is the protection of MBs from resource exhaustion attacks. Transparent MBs can add puzzle challenges to packets [20], [21], however this charges the peers. Non-transparent MBs are protected by built-in puzzle mechanisms during the registration process, and may use message origin authentication for binding IPsec traffic to the registered peer.

In our signaling scheme UFA_GWs behave as traffic relays or non transparent MBs that map traffic from one IPsec tunnel to another IPsec tunnel based on the inner headers that contain the HITs. The inner header causes overhead on the one hand, but easily solves traffic flow binding problems.

G. 802.21 Media Independent Handover (MIH) protocol

The IEEE 802.21 [5] protocol specifies a unified framework for proactive handover control in heterogeneous architectures (i.e., 802.3, 802.11, 802.16, 3G networks). It supports event and command service (ES, CS) mainly used for local and remote link-layer event monitoring, and information service (IS) collecting static information on access networks. The previous services enable network and MN-controlled handover decisions, i.e., target L2 Point of Access (PoA) selection. The standard defines procedures for PoA resource availability checks, resource reservation, and release. The handover execution protocols and decision algorithms are outside the scope of the standard. Point of Services (PoS) are network elements that communicate directly with the MN, and can assist in handover decision.

For our signaling scheme, UFA_GWs are PoS, but often non-PoA entities (i.e., no Layer 2 link is available between the MN and the non-PoA UFA_GW).

III. Fundamentals of HIP-based Ultra Flat Architecture

A. General architecture of HIP-based UFA

Our proposal for a HIP-based Ultra Flat Architecture is depicted in Fig. 1. The architecture comprises 1) several access networks (both wired and wireless), 2) an IP/MPLS transit network, 3) an IEEE 802.21 MIH management subsystem and 4) a HIP-based control network. To address issues drawn in Section I, centralized IP anchors between Point of Access (PoA) nodes and correspondent nodes are removed, and network functions are placed at the edge of the transit and access networks (close to the Point of Access (PoA) nodes) in the Ultra Flat Architecture Gateways (UFA_GWs). UFA_GWs control the procedures described in Section IV.

Heterogeneous access networks provide the air interface for MNs making them able to connect to the core infrastructure (and to the Internet) anytime, anywhere. Besides to support IEEE 802.21 mechanisms there are no other restrictions regarding the access technologies to be used in this framework: any kind of access system can be applied in any kind of heterogeneous setup.

The IP/MPLS transit network is the operator's backbone including routers and core network elements (for service and configuration provision, 802.21 services etc.), and natively connecting UFA to the global backbone (i.e., to the Internet). Locators used in the transit network are *global locators* while locators in the access networks are *local locators*. UFA_GWs are 1) performing fast HIP-level access authorization (see III-B1), and 2) actively interacting with hosts through delegation-based HIP and IPsec association management and context transfer (see III-B2) for optimized message exchange in HIP-based UFA mobility and multihoming operations. Our proposed framework transports end-to-end flows between MNs and CNs in a hop-by-hop manner. The middle-hops are the UFA_GWs, i.e., the delegates of the end peers. Hence task 4) of the UFA_GWs is performing the actual mapping/routing between outer header IPsec tunnels based on inner header identifiers. We propose the use of HITs in inner IP headers for the identification of flows, with the same purpose as the Control Plane Header (CPH) in [15]. Without delegation, maintaining end-to-end security associations (SAs) between every communicating peers would be required, as in the SPINAT-based frameworks [15]. Note, that there is a trade-off between the delegation-based and SPINAT-based alternatives, i.e., the first alternative introduces an extra-header in every packet, but reduces signaling at the MNs, the second requires SPINAT-based middleboxes, i.e., UFA_GWs, and MN-initiated signaling for the maintenance of a high number of HIP and IPsec associations.

The IEEE 802.21 MIH management subsystem handles handover preparation issues and relating signaling tasks in order to initiate proactive HIP handover procedures in the UFA and to support network and mobile controlled handover decision. UFA_GWs are PoS, but often non-PoA entities. According to the standard, UFA_GWs must communicate over

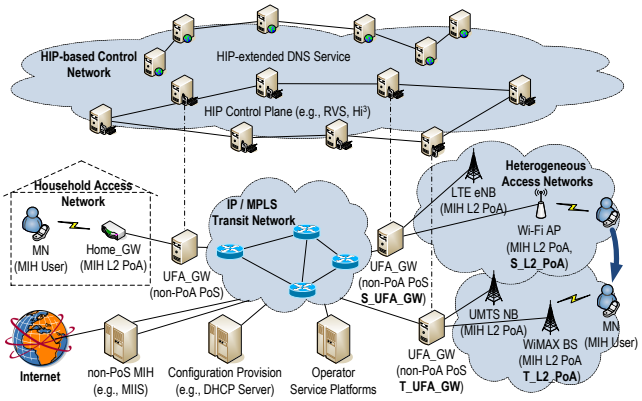

Fig. 1. HIP-based Ultra Flat Architecture.

Reference Point 5 (RP5) with PoAs and over RP3 with MNs. In our signaling scheme, network initiated 802.21 handover preparation procedures are triggered by the serving UFA_GWs (refer to Appendix C.2 in [5]). RP3 and RP5 messages are sent over L3 [22], and protected by HIP and IPsec.

The control network in the upper part of Fig. 1 contains a HIP-compatible Domain Name System [23] for resolving domain names to host identities and/or locators depending on the actual situation. In addition there is the HIP Control Plane which stores and distributes dynamic and presumably frequently changing binding information between host identities and locators of all actively communicating (mobile) hosts in UFA. This control plane might be a conventional RVS [9] park or a complete distributed HIP signaling architecture like Hi^3 [7]. The records managed here are provided by the UFA_GWs using their own global locators as location information to be bounded with identities of their actively interacting partners.

B. Proposed HIP extensions

1) Fast access authorization on HIP-level: In UFA one design issue is to avoid duplicate authentication procedures with remote AAA servers on L2 and HIP level. In operator-based environments, the network access authentication on L2 involves the AAA server (and HSS) in the core network. We suppose that L2 access authorization builds upon an EAP authentication method, such as the EAP-AKA or EAP-SIM [24]. We also suppose that EAP Re-authentication Protocol (ERP) [25] is deployed using local or home EAP re-authentication (ER) servers to provide fast L2 re-authentications when the MN moves to a new EAP authenticator. Note, that in our reference scenario, L2 PoAs contain the EAP authenticator, the home AAA server includes the EAP server and the EAP re-authentication server. The UFA_GW may include the local ER server. Fig. 2 illustrates the access authorization concept for the UFA. It illustrates the prerequisites and the functioning of our proposed HIP-level access authorization. Our proposal requires the introduction of new HIP notification parameters, and two EAP message types, as shown in the final message exchange between the MN and the local ER server. Moreover,

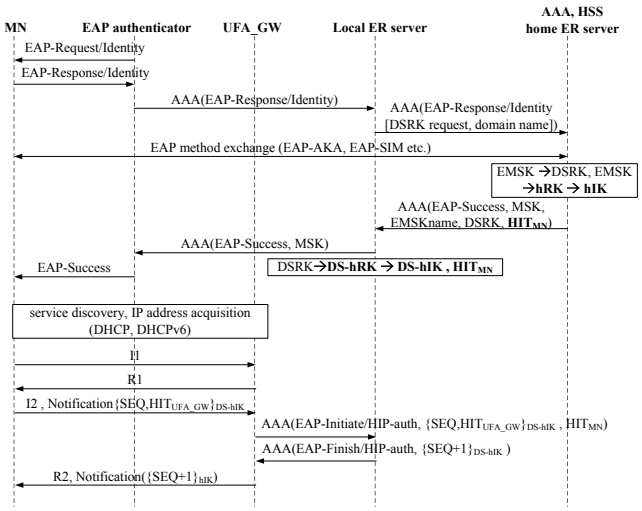

Fig. 2. Access authorization.

we define a new key hierarchy to generate cryptographically separate keys from the session keys provided by ERP and EAP L2 authentications. The Extended Master Session Key (EMSK) is created after a successful EAP authentication, assuming that it is supported by the chosen L2 EAP authentication method. The EMSK can be used to create usage specific root keys (RK) for any purpose. We propose to create a new usage specific root key for HIP-level peer authorization, according to [26]. A HIP peer authorization root key (hRK) is derived from the EMSK or from the Domain Specific Root Key (DSRK) in home and local ER servers, respectively. The DSRK is derived by the home ER server based on the local ER domain name and the EMSK [26]. DSRK is transfered from the home server to the local ER server in the EAP-Success message. AAA protocols, such as Radius or DIAMETER, support EAP transport between the authenticator and the local and home ER servers. Between the MN and the authenticator the EAP transport is L2-specific.

From the HIP root key (hRK), a HIP integrity key (hIK) is derived. This is used to mutually authenticate, i.e., prove the possession of hRK, between the MN and the local ER server during HIP BEX. The MN's access authorization can be checked by the local ER server because it knows the expected HIT_{MN} from the home server's EAP-Success message, and the MN proves to know hIK. The local ER's authenticity is proved to the MN by using the correct hIK. The MN checks the freshness of the reply using a sequence number that is known only by the MN and the local ER server. The UFA_GW is authorized by the MN, because it proves to be in trust relationship with the local ER server. HIP provides integrity, message-origin authentication, and freshness for I2 and R2 messages.

Note that further master session keys (hMSKs) could be derived from hRK. This could replace the Diffie-Hellman key exchange during HIP BEX, because the MSKs could be used to calculate transient session keys for the HIP and IPsec associations between the MN and the UFA_GW.

If there is no local ER server, the home ER server can also be reached by the UFA_GW. Local ER servers derive domain specific HIP peer authorization root keys (DS-hRK) from DSRK, while home ER servers derive HIP peer authorization root keys (hRK) from the EMSK.

2) HIP-based delegation services: Two novel HIP-based delegation service types –the bedrocks of our HIP-based UFA signaling scheme– are presented in this section. On one hand they will help us to reduce the number of DH key exchanges and puzzle solutions in user equipments by decreasing number of HIP BEXs between communicating end terminals. On the other hand delegate UFA_GWs remove overhead from wireless links by shifting significant part of signaling overhead of MNs from the air interface to the wired UFA segment. Both of the defined HIP delegation service types require preliminary registration procedure called Delegation Establishment as depicted in the upper part of Fig. 3. An existing HIP and IPsec association (i.e. completed BEX) is presumed between the Delegator and the Delegate or must be created upon the Delegation Establishment. Also both services rely on the messages and parameters drafted in Tab. I.

In case of *Type 1 Delegation* (Fig. 3) states are established through the Delegate but maintained directly by the Delegator after context transfer. Here, the Delegator asks the Delegate to establish HIP and IPsec states between Delegator and specified nodes (CNs), and then transfer established states from Delegate to Delegator. The existing IPsec and HIP associations between the Delegate and the CN must not be deleted or moved: it provides a base for creating the new IPsec and HIP associations between the Delegator and the CN. It is important that SPI collision is to be avoided at the Delegator and the CNs, not at the Delegate (that is why the Delegator sends its favorable SPI range). The created states are transferred to the Delegator using CTXP messages [16] over the presumed IPsec SAs.

In our HIP-based UFA scheme, this delegation type is employed during handover execution when T_UFA_GW will ask S_UFA_GW to create states between itself and the MN and MN's peer nodes.

In case of *Type 2 Delegation* (Fig. 4) the Delegator requires the Delegate to establish HIP and IPsec states for itself at specified peer nodes and also asks the Delegate to further maintain the created local states. During this type of delegation, SPI collision is to be avoided at the Delegate and the CNs side (not at the Delegator), however it is handled by basic HIP mechanisms.

In HIP-based UFA, this delegation type is applied for HIP and IPsec association establishment between the MN and a CN or the MN and an RVS. Here the UFA_GW is the Delegate of the MN in order to maintain HIP and IPsec states on behalf of its Delegator. During handover execution, location update at CNs for MN is initiated by the T_UFA_GW: in that case the T_UFA_GW acts as a Type 2 Delegate of the MN and the S_UFA_GW. Here we capitalize the feature that Type 2 Delegation service enables indirect authorizations, i.e., the use of certificate-chains. E.g., if a T_UFA_GW does not

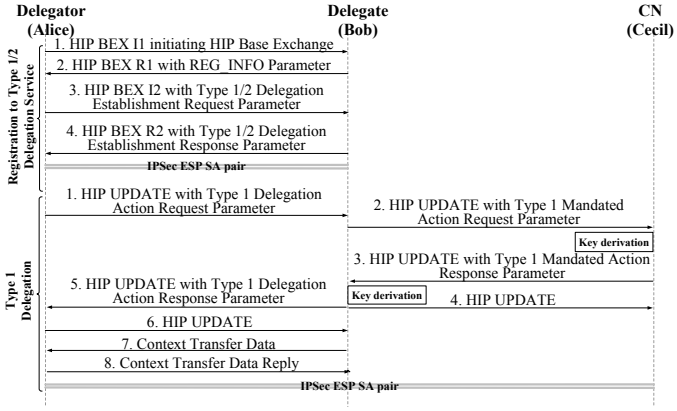

Fig. 3. Registration to Type 1/2 Delegation Service and requesting Type 1 Delegation Service.

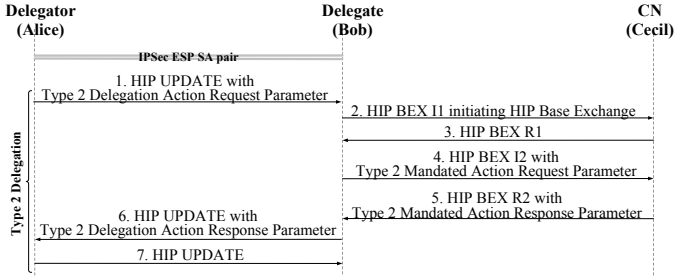

Fig. 4. Requesting Type 2 Delegation Service.

have the authorization certificate of MN, it may still have an authorization from the S_UFA_GW, while the S_UFA_GW has the MN's authorization.

IV. Main procedures of HIP-based UFA

The steps of the terminal attachment, session establishment, and handover execution procedures are briefly summarized in this part due to space limitations. Terminal attachment procedure contains: 1) L2 attachment of the MN to the L2 PoA using an EAP based authentication providing EMSK. 2) bootstrapping the MN, service discovery. 3) HIP BEX between the MN and the serving UFA_GW. Peer authentication is provided by HIP BEX, but their authorization information is mutually checked through the local (or home) ER server. As a following step, 4) the MN registers to Type 2 Delegation service at the UFA_GW and issues an authorization certificate to it. 5) UFA_GW registers the MN to the RVS service due to the delegation. 6) 802.21 service management requests are sent from the UFA_GW PoS to the MN, to subscribe to MN's link layer events.

Session establishment between the MN and a CN is basically a Type 2 Delegation service where the Delegator, the Delegate and the CN are the MN, MN's UFA_GW and the CN, respectively. If the CN is also an MN, then the HIP and IPsec association is established with the UFA_GW of the CN, and CN is notified using HIP Notification in order to create HIP association states with the MN in the CN. The UFA_GW also creates a traffic mapping table entry for the MN and the CN in order to route their traffic into the appropriate IPsec tunnels.

Handover execution contains the following sub-procedures: 1) 802.21 handover preparation initiated by the S_UFA_GW. At the 802.21 commit phase the S_UFA_GW sends a Type 2 Mandated Action Request to the T_UFA_GW for handing off the MN and its ongoing sessions. In this request the S_UFA_GW sends information on the current peers of the MN to the T_UFA_GW. 2) The T_UFA_GW selects the peers with which it has not established HIP and IPsec associations. 3) The T_UFA_GW sends a Type 1 Delegation Action Request to the S_UFA_GW to create HIP and IPsec associations between the delegator and the selected peers, including the MN. Note, that neighboring UFA_GWs have pre-established HIP and IPsec associations, and have registered to other's Type 1 delegation service. After successful state creation the S_UFA_GW exchanges the HIP and IPsec states to the T_UFA_GW in CTD/CTDR message sequence. 4) The T_UFA_GW creates HIP associations in the name of the MN with the peers of the MN using Type 2 Mandated Action Requests. The T_UFA_GW at this time is either directly or indirectly authorized by the MN. Direct authorization might be obtained from the MN after Type 1 Mandated Action Request/Reply sequence between the MN and the S_UFA_GW, and the context transfer (i.e., in step 3). In case of indirect authorization the T_UFA_GW has a Type 2 delegation service authorization certificate chain involving the S_UFA_GW. 5) The T_UFA_GW creates traffic mapping in order to route data packets between the MN and its CNs.

V. Evaluation

Compared to the SIP-based alternative published in [2], [3] and [4], the HIP delegation-based scheme is slightly better regarding the service interruption time caused by hard handovers. In our scheme, the service interruption time only contains the local link activation delay of the MN. HIP and IPsec contexts are proactively established. In the SIP-based alternative, after the L2 attachment of the MN to the target L2 PoA, one SIP re-invite message must be sent from the MN to the target UFA_GW. Considering the one-way delay of current access technologies, both alternatives perform below the 200 ms requirement for real-time service interruption delay.

The SIP-based alternative performs better than HIP-based regarding signaling overhead. Both alternatives must fulfill the same functionalities. However, HIP applies 3-way handshakes, instead of the 2-way handshakes in the SIP-based alternative. In 3-way handshakes the third HIP Update message is an acknowledgment message, which is sent from the initiator to the responder. It assures the responder about the fact that the initiator got the second HIP update message.

HIP is better in security than SIP-based alternative due to the 3-way handshakes and the built-in DoS resistance on HIP level. Both alternatives provide mutual authentication and data protection between the MN and the UFA_GW. Currently, the path between the MN and the UFA_GW is

TABLE I
EXPLANATION OF HIP-BASED DELEGATION SERVICE MESSAGES.

HIP Parameter	Description
Delegation Establishment Request	The Delegator sends to the Delegate for itself or on behalf of another node in order to request Type 1/2 delegation service using HIP REG_REQ parameter. Authorization Certificate chain of the acquiring node must be included in HIP NOTIFICATION parameter(s).
Delegation Establishment Response	The Delegate sends to the Delegator in order to acknowledge or reject Type 1/2 delegation service establishment using HIP REG_RESP or REG_FAILED parameter.
Delegation Action Request	The Delegator sends to the Delegate for itself or on behalf of another node in order to request HIP and/or IPsec association creation or update. In case of Type 1 Delegation Service the state information will be transfered to the Delegator. For Type 2 Delegation Service, the states resulted by the action will be created and further maintained by the Delegate.
Delegation Action Response	The Delegate sends to the Delegator in order to report the Type 1/2 delegation action results in HIP NOTIFICATION parameter(s).
Mandated Action Request	The Delegate sends to 3^{rd} party node(s). For Type 1 Delegation Service HIP and/or IPsec associations will be created by the Delegate and transfered to the Delegator. In case of Type 2 Delegation Service, new HIP and/or IPsec states are created on behalf of the Delegator by the Delegate and/or traffic mapping rules will be updated. HIP NOTIFICATION parameters are used to transfer the required information such as supported IPsec SPI values of the Delegator, global locator(s) of the Delegator, list of supported HIP and IPsec transforms, traffic mapping rules, Delegator peer list, configuration and service registration parameters, etc.
Mandated Action Response	3^{rd} party node(s) send to the Delegate in order to report Type 1/2 mandated action results in HIP NOTIFICATION parameter(s).
Context Transfer Data (CTD)	Sent by the Delegate to Delegator, and includes feature data (i.e., HIP and IPsec context data).
Context Transfer Data Reply (CTDR)	Sent by Delegator to Delegate, indicating success or failure of context transfer.

considered as the most vulnerable part of the network. The UFA architecture is intended to be applied by operators, hence appropriate network-domain security measures are expected. HIP-based alternative is also prepared for scenarios where the UFA_GWs are located in untrusted networks, due to the HIP applied as network-domain security control protocol between the UFA_GWs. IPsec associations providing null encryption may be used in the network domain within trusted operator networks.

Basically, both alternatives use separate IDs and locators. The SIP and HIP alternatives apply SIP URIs and HITs to refer to identities, respectively. HIP host identifiers are self-certifying that reduces the complexity of the authorization procedures. HIP-based alternative can not only be used by SIP-based applications (e.g., for IMS services), but by any application, e.g., legacy internet applications. The deployment complexity of the HIP-based alternative is much higher than in case of the SIP-based alternative. While SIP requires application level changes in the MNs, CNs, and UFA_GWs, and IMS naming services can be reused, the HIP-based scheme requires the deployment of HIP protocol in all participating parties, i.e., MNs, CNs, UFA_GWs. HIP also requires new naming service, e.g., HIP-capable DNS and RVS, to resolve HITs to locators.

VI. DISCUSSION AND CONCLUDING REMARKS

In this paper, we have introduced a new delegation-based HIP signaling scheme for the UFA and compared to an existing SIP-based alternative. The results show that our scheme is able to support legacy internet applications in an operator based environment, it is stronger in security, but its deployment requires more additional modules in the architecture. For IMS applications, SIP-based alternative is a better choice. We have introduced two novel HIP delegation services for optimization reasons between the MN and the UFA_GW. We proposed a new usage type for root keys that should be derived from the EMSK, i.e., the HIP peer authorization root key, in order to provide fast re-authentication on HIP level. Hence we eliminate redundant message exchanges with the home AAA server throughout terminal attachment and periodic re-authentications.

Several issues remain open, or could not be written due to space limitations. We plan to evaluate the trade-off between SPINAT-based and delegation-based architectures; the first requiring many end-to-end SAs and SPI collision avoidance, the second requiring public-key certificate issuance from the delegators and causing message overhead due to the application of inner IP headers bearing the HITs of the peers of the end-to-end sessions. Another plan is to evaluate the gain of delegation and context transfer based handovers related to complete state re-establishment. Our scheme is open to provide per-application mobility, using Security Policy Database (SPD) entry registrations in peers. Furthermore, session mobility services could be based on Type 1 HIP delegation service, if we imagine that the the previous and next terminals act as the Delegate and the Delegator, respectively.

ACKNOWLEDGMENT

Ultra Flat Architecture is being studied in P1857 Eurescom project and interests France Telecom, Portugal Telecom and Mobile Innovation Centre Hungary. The authors would like to express their appreciation to the many individuals whose participation in the project made this research possible, especially to Philippe Herbelin, Khadija Daoud, Pedro Miguel Neves, and Szabolcs Nováczki.

REFERENCES

[1] ITU-T, "General requirements for ID/locator separation in NGN," ITU-T Draft Recommendation, ITU-T Y.2015 (Y.ipsplit), Feb. 6, 2009.

[2] K. Daoud, P. Herbelin, and N. Crespi, "UFA: Ultra Flat Architecture for high bitrate services in mobile networks," in *Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008*, Cannes, France, Sep. 15–18, 2008, pp. 1–6.

[3] ——, "One-Node Based Mobile architecture for better QoS control," in *Proceedings of the 1st IFIP Wireless Day Conference 2008*, Dubai, UAE, Nov. 24–27, 2008, pp. 1–5.

[4] K. Daoud *et al.*, "Performance and Implementation of UFA: a SIP-based Ultra Flat Mobile Network Architecture," in *Proceedings of PIMRC 2009*, Tokyo, Japan, Sep. 13–16, 2009, pp. 1–6.

[5] IEEE, "IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover," IEEE Std 802.21-2008, Jan. 2009.

[6] R. Moskowitz *et al.*, "Host Identity Protocol," RFC 5201, Apr. 2008.

[7] A. Gurtov *et al.*, "Hi3: An efficient and secure networking architecture for mobile hosts," *Journal of Computer Communications*, vol. 31, no. 10, pp. 2457–2467, 2008.

[8] J. Laganier, T. Koponen, and L. Eggert, "Host Identity Protocol (HIP) Registration Extension," RFC 5203, Apr. 2008.

[9] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension," RFC 5204, Apr. 2008.

[10] S. Heikkinen and H. Tschofenig, "HIP based Approach for Configuration Provisioning," in *Proceedings of the IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06)*, Helsinki, Finland, Sep. 11–14, 2006, pp. 1–5.

[11] J. Ahrenholz, "HIP DHT Interface," IETF Draft, Nov. 2009.

[12] I. Baumgart, "Peer-to-Peer Name Service (P2PNS)," IETF Draft, Nov. 2007.

[13] G. Camarillo *et al.*, "HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking," IETF Draft, Jan. 2010.

[14] P. Nikander and J. Melen, "A Bound End-to-End Tunnel (BEET) mode for ESP," IETF Draft, Aug. 2008.

[15] J. Ylitalo, P. Salmela, and H. Tschofenig, "SPINAT: Integrating IPsec into Overlay Routing," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05)*, Athens, Greece, Sep. 5–9, 2005, pp. 315–326.

[16] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol (CXTP)," RFC 4067, Jul. 2005.

[17] F. Allard and J.-M. Bonnin, "An application of the context transfer protocol: IPsec in a IPv6 mobility environment," *International Journal of Communication Networks and Distributed Systems*, vol. 1, no. 1, pp. 110–126, 2008.

[18] P. Nikander and J. Arkko, "Delegation of Signalling Rights," in *Security Protools*, ser. Lecture Notes in Computer Science, B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, Eds. Springer, 2004, vol. 2845, pp. 575–586.

[19] J. Melen *et al.*, "Host Identity Protocol-based Mobile Router (HIPMR)," IETF Draft, May 2009.

[20] T. Heer *et al.*, "End-host Authentication and Authorization for Middleboxes based on a Cryptographic Namespace," in *In Proceedings of the IEEE International Conference on Communications Symposium 2009 (ICC 2009)*, Dresden, Germany, Jun. 14–18, 2009, pp. 1–6.

[21] ——, "End-Host Authentication for HIP Middleboxes," IETF Draft, Feb. 2009.

[22] T. Melia *et al.*, "IEEE 802.21 Mobility Services Framework Design (MSFD)," RFC 5677, Dec. 2009.

[23] P. Nikander and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extension," RFC 5205, Apr. 2008.

[24] 3GPP, "3G Security; Wireless Local Area Network (WLAN) interworking security," TS 33.234, Mar. 2010.

[25] V. Narayanan and L. Dondeti, "EAP Extensions for EAP Reauthentication Protocol (ERP)," RFC 5296, Aug. 2008.

[26] J. Salowey *et al.*, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," RFC 5295, Aug. 2008.